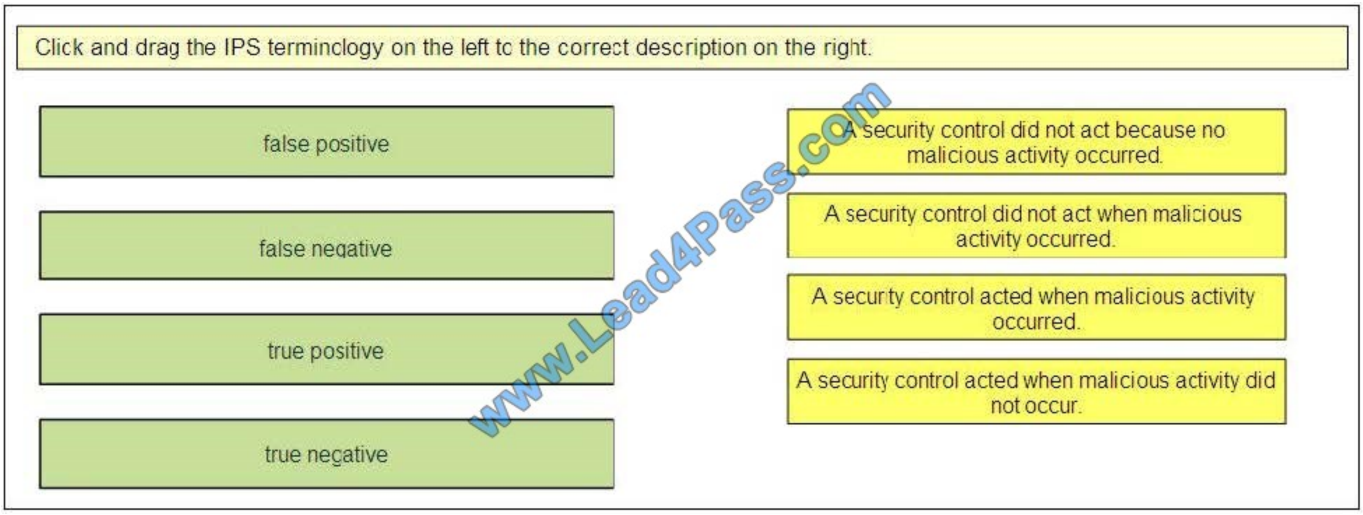
642-627 Q&As

Implementing Cisco Intrusion Prevention System v7.0

QUESTION 1

Select and Place:



Click and drag the IPS terminclogy on the left tc the correct description on the right.

false positive

false negative

true positive

true negative

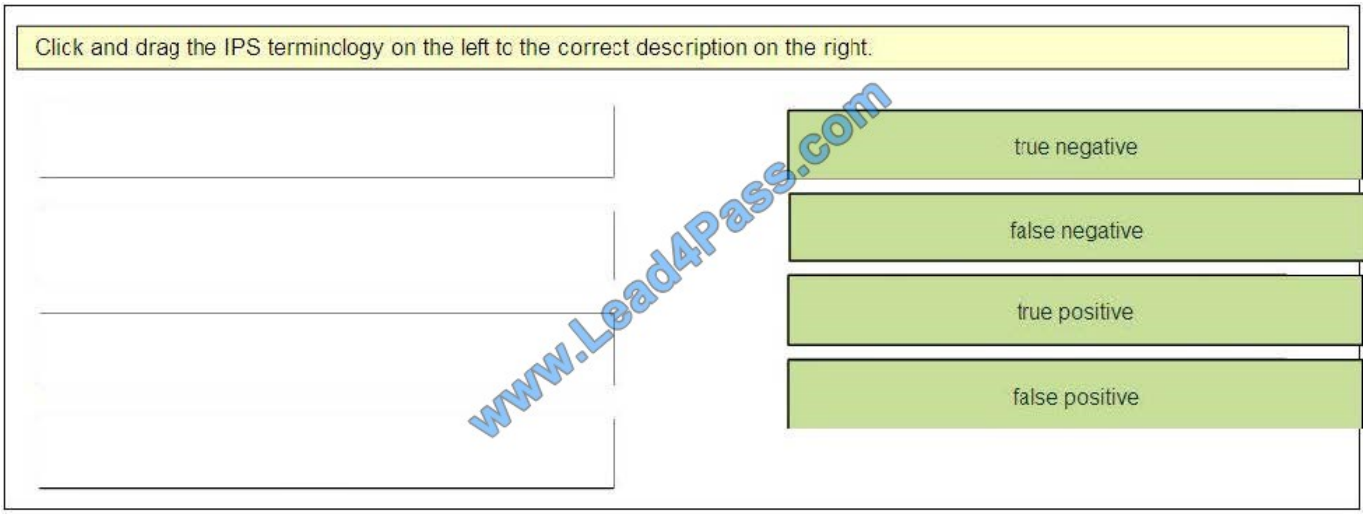
A security control did not act because no malicious activity occurred.

A security control did not act when malicious activity occurred.

A security control acted when malicious activity occurred.

A security control acted when malicious activity did not occur.

Correct Answer:



Click and drag the IPS terminclogy on the left tc the correct description on the right.

true negative

false negative

true positive

false positive

QUESTION 2

What must be configured to enable Cisco IPS appliance reputation filtering and global correlation?

A. DNS server(s) IP address

B. full sensor based network participation

C. trusted hosts settings D. external product interfaces settings

Correct Answer: A

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/ime/ime_collaboration.html

Global Correlation Requirements

Global correlation has the following requirements:

?alid license

You must have a valid sensor license for global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted.

Once you install a valid license, the global correlation features are reactivated.

?gree to network participation disclaimer

?xternal connectivity for sensor and a DNS server

The global correlation features of IPS 7.0 require the sensor to connect to the Cisco SensorBase Network.

Domain name resolution is also required for these features to function. You can either configure the sensor to connect through an HTTP proxy server that has a DNS client running on it, or you can assign an Internet routable address to the

management interface of the sensor and configure the sensor to use a DNS server. In IPS 7.0 the HTTP proxy and DNS servers are used only by the global correlation features.

QUESTION 3

Which three of these are true with respect to the numeric values associated with the target value rating? (Choose three.)

A. Mission Critical = 100

B. Mission Critical = 200

C. High = 75

D. Medium = 50

E. Low = 75

F. 100 is the default target value rating

Correct Answer: BEF

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd806e7299.html

QUESTION 4

The Cisco IPS appliance anomaly detection signatures cover which three protocols? (Choose three.)

A. TCP

B. ICMP

C. UDP

D. NETBIOS

E. IP

F. other

Correct Answer: ACF

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/idm/idm_anomaly_detection s.html#wp2040302

Anomaly Detection Signatures

The Traffic Anomaly engine contains nine anomaly detection signatures covering three protocols (TCP, UDP, and other).

QUESTION 5

Which four networking tools does Cisco IME include that can be invoked for specific events, to learn more about attackers and victims using basic network reconnaissance? (Choose four.)

A. ping

B. traceroute

C. packet tracer

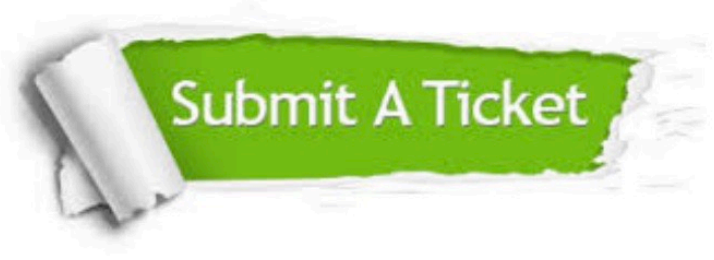
D. nslookup

E. whois

F. nmap

Correct Answer: ABDE

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/ime/ime_getting_started.htm l IME also supports tools such, as ping, trace route, DNS lookup, and whois lookup for selected events


Submit A Ticket